International Journal of Applied and Physical Sciences
volume 9 pp. 1-8 doi: https://dx.doi.org/10.20469/ijaps.9.50001

Bioengineering/ Biomedical Engineering Interlink with Internet of Medical Things and Legal Hitches

Nanda Pardhey*
School of Law,
University of Petroleum and Energy Studies,
Dehradun, India.

Abstract: Bioengineering due to advancement in technological innovation has grown and expanded its horizons in various allied field but this paper will deal with biomedical engineering, and it's interlinked with Internet of Medical Things (IoMT) its applicational concerns and issues relating to lack of standardization and regulation of IoMT across the world. Herein the paper the author firstly will discuss about the distinction and interrelationship between bioengineering and biomedical engineering and how they are overlapping with each other. Bioengineering is a broader canopy that encompasses various allied fields within itself of which biomedical engineering is one. Due to technologically innovative advancement because of Internet of Things (IoT) rapid growth that has been adapted in medical health care sector too and medical healthcare sector are using varied IoMT devices that had eased the functionality of medical professionals but at the same time had raised various concerns and challenges pertaining to data security, cybersecurity, privacy, and confidentiality. Medical professionals are regulated strictly nationally and internationally but regulation of IoMT is challenging due to lack of standardize practices, policies and procedures not at place, lack of trained IoT medical professionals and when such devices connected with internet networks that may faces data breaches which could risk the data that could be tampered, privacy infringement when not authorized and how it shared at different levels could lead concerns about IoMT. Biomedical devices preventive and protective measures mechanisms could be place are dealt.

Keywords: *Biomedical engineering, healthcare, IoMT, Security, challenges, legal regulation, and remediation*

Received: 05 February 2023; ***Accepted:*** 10 April 2023; ***Published:*** 12 June 2023

I. INTRODUCTION

In last two decades technology has grown in leaps and bound. Technology has made eminent changes in the structure and results of original product or has brough remedial changes in results in the outcome product. Technology of Bioengineering and Biomedical engineering also has seen developments that are gaining grip in the industries and providing solutions to the day-today life issues by use of engineering. Bioengineering/biomedical engineering education is a social process integrating accrued knowledge, expertise, and values pertaining to a fusion of engineering sciences and biomedical sciences that have been disseminated across generations [1]. Understanding of bioengineering and biomedical engineering is important to observe the growth it has gained in past few years [1]. Before moving ahead with these two concepts it require to be expounded for better understanding of these two terminologies are they similar or distinct from each other, bioengineering and biomedical engineering considered as one but there have been inconsistencies in interpretation of these two terminologies by the professional those are utilizing them. Certain professionals and authorities working in field of bioengineering considered bioengineering as broader umbrella which covers different bioengineering within themselves which cover the ambit of biological engineering of human, animal and

*Correspondence concerning this article should be addressed to Nanda Pardhey, School of Law, University of Petroleum and Energy Studies, Dehradun, India. E-mail: npardhey@ddn.upes.ac.in

plants, biomedical engineering that relates to the combination of relating to both biology and medicine together and medical engineering that specifically in medical sector known as *'Clinical Engineering'*. Moreover, largely bioengineering is considered as 'basic research which related to biology and technology i.e., known as *'biotechnology'* commonly now and genetic engineering. Looking on the various interpretation it could be said that bioengineering in practice is broader umbrella that encompasses other fields and therefore, it could be interpreted that bioengineering and biomedical engineering has co-existence and co-relation with each other and there is existence of close degree of overlap between them. Let's, understand the definition and meaning of both the concepts for better comprehension of the two terminologies.

'Bioengineering' through which an application of engineering and its principles are utilized to improve various disease prevention and protection or providing a treatment, through biological biotechnology/bioengineering agricultural production are improved, edited with desired traits, nutrition, colour flavour etc., energy sustainability by using bioengineering and more area wherein bioengineering is used for sustainable development. Bioengineering which understands the physiological and biological function that improves the comprehensively and integrate the living organisms' function and resolve its issues. The working "definition of Bioengineering according to the National Institutes of Health, Bethesda, MD, USA, is (Anonymous, 1997): "Bioengineering integrates physical, chemical, or mathematical sciences and engineering principles for the study of biology, medicine, behavior, or health. It advances fundamental concepts, creates knowledge for the molecular to the organ systems levels, and develops innovative biologics, materials, processes, implants, devices, and informatics approaches for the prevention, diagnosis, and treatment of disease, for patient rehabilitation, and for improving health"" [1]. Bioengineering is usually defined as a basic research-oriented activity closely related to biotechnology and genetic engineering, that is, the modification of animal or plant cells, or parts of cells, to improve plants or animals or to develop new microorganisms for beneficial ends [2].

Biomedical Engineering (BME) that is used to find solutions biological and medical issues and problems which can improve healthtretment medications, improve health care of patients by using standard healthcare instruments that are viable and pain-relieving. Bioengineering and Biomedical engineering object is to improve the healthcare sector by improving existing devices in medical sector or the processes through which a patient is given treatment by advance bioengineered diagnostics. Bioengineering in medical field or biomedical engineering has developed with science and technology that has acclaimed all over world and various treatments or diagnosis and treatment provided, new methods of surgical instruments innovated through use of biomedical engineering or various methods of imaging for detection of ailment/diseases, development of new methods or material for treatment by use of genetic engineering rDNA methods, tissue engineering and macromolecular engineering commonly known as 'Protein/DNA' which is developed to cure that has been spurred and taken healthcare sector advancements through technology in medicine and biology. Recently, healthcare practices have been steered towards new emerging frontiers, including, among others, functional medical imaging, regenerative medicine, nanobiomedicine, enzyme engineering, and artificial sensory substitution [1].

II. PRACTICAL AREA OF BIOENGINEERING/ BIOMEDICAL ENGINEERING

Biomedical engineering utilization is done to design medical devices for treatment or create a system that would repair or monitoring or assist in treatment that assist the functions of human body. Through biomedical engineering in the healthcare sector in with hi-tech super speciality hospital they replicate nature's technique which is called biomimetics through medical device or therapy to limited extent due to regulation by regulatory bodies across the globe. Though in a regulated manner they have been developed and research in this area is ongoing which study the structural biology which could involve in persons tissue or developing organ regeneration. Biomedical engineering used in following areas:

- Cells are programmed by their genetic code to build the tissues and organs of our bodies [3]
- Cells produce proteins, polysaccharides, glycoproteins, and lipids that self-assemble into composite extracellular matrices that have multiple diverse forms and serve to support tissue growth [3]
- Cells communicate via growth factors and their recruitment, and even cellular fate is determined by protein signals [3]
- Blood vessels play a crucial role in tissue growth by providing nutrients, a means for waste removal, and a supply of additional cells to support further growth [3].

Biomimetic paradigms that have been derived from these basic structural and developmental biology concepts provide a rational starting point for the design and fabrication of biomaterials, especially for regenerative tissue-engineered medical devices [3].

Biomedical engineering has worked as miracles for various cell therapies that are used for human cells which act as therapeutic agents that had shown to alleviate a pathological condition of the patients through use of bio-engineering/biomedical engineering. Blood transfusion is one such old cell therapy that being used from last two decades or more as therapeutic treatment are legally recognized and been beneficial and shown successful results for years through biomedical engineering. Anemic patients through this technology are treated by red blood cells (RBCs) as transplant that helps the patient to restore their adequate oxygen transport in their body. Whenever any patient faces blood clotting issues that their platelets are transfused. Same way there are various biomedical engineering treatments like Bone marrow transplantation (BMT), transplants that are xenogeneic or Xenotransplantation taking place wherein the donor and the person who is recipient are members of different species or allogenic are one who are similar types but not genetically identical/matching or syngeneic where they are genetically similar/ identical as in case of identical twins. Regenerative medicine offers potential new therapies through the bioengineering of female reproductive tissues [4]. Bioengineering approaches have demonstrated enormous potential in treating female infertility, which can be broadly classified into whole organ transplant and tissue engineering approaches [5].

Likewise, there are in recent times various inventions and innovation done in biomedical engineering like In-Vitro Fertilization (IVF) technique is the result of biomedical engineering wherein infertile couple can have child through the advance technology, Artificial Intelligence in medical imaging, Prosthetics, from dentures to artificial limbs, Robotic and laser instruments to assist in surgeries to doctors, Radiation therapy, Genome editing, Wearable medical devices (for e.g. day-today activities and Fitness Trackers for patients, commonly used Smartwatches for fitness, Electrocardiogram (ECG) monitors, Blood Pressure (BP) monitors, for ladies specifically during their pregnancy used Pregnancy monitor, etc. to name the few).

III. INTERNET OF MEDICAL THINGS (IOMT) INTERFACE WITH BIOMEDICAL ENGINEERING

Technological advancement through internet which clubbed with science innovation brought in healthcare sector through Internet of Medical Things (IoMT) which has revolutionized altogether the old medical practices and procedure wherein medical devices used on patients and their application relate to Information Technology (IT) systems using online computer networks in healthcare. Biomedical engineering with IoMT had brough major changes in the treatment and diagnostic methodology of the patients wherein many inventions are made that are equipped with advanced technology which enable to captures and store patients' information and data that their physicians can use that would recover and improve their patient's care and treatment process. Advance and new IoMT with biomedical engineering is helping to shape medical sector, health care industry and awareness and growth of consumer devices used by them for detection, treatment, and diagnosis. Biomedical engineering, we can say has adapted with IoMT now widely used in healthcare that are considered cost effective, easy application process, data accuracy and data security for doctors and hospitals. Few real-time heart monitoring systems is developed those are to be considered as being cost effective, easy to apply, accuracy or precision in result, and to some extend data security. Various monitoring systems and devices for healthcare sector as follow:

A. Real-time patient health monitoring & Patient wearable devices

The most promising application is in real-time monitoring of chronic illnesses such as cardiopulmonary disease, asthma, and heart failure in patients located far from the medical care facilities through wireless monitoring systems [6]. Due to increasing number of heart attack patients and the rate that is increasing day-by-day so the doctors use for such cardiac patients real time health monitor which keep a tab on their heart rate, temperature and BP that could be traced by wearable sensors or through android apps which are commonly used now to acquire data through android listening port which help to receive patients information that created through port and store that medical information which is usually automatically transmitted to web interface using wireless devices of communication that could help the doctors to know the medical status of the patient with their location information in real-time and all such information is store in the server which is available at click to the doctor at his place. The integration of wearable devices those can be connected directly to the individual's mobile networks had shown potentials in past few years that has increased rapid usage of wearable devices those show results instantly, somewhat reliable to some extent and easily transfer of information from the patient to the doctors. The system measures the parameters in real-time and displays on the LCD and in the cloud which enables monitoring of patient health when the doctor is with the patient or wireless monitoring for any place [7].

B. Ventilators

It's a device that used to patients who faces respiratory distress and during Covid-19 commonly were used during such patients. Ventilator's function is to exhale gas through the machine into patient role lung and helps them to strengthen and fix the issue faced by patient which has malfunction of respiratory organs/muscles. Through use of IoMT the process of monitoring and controlling the much needed ventilator for COVID-19 patients when there is pandemic or epidemic outbreak, that could be helpful and possible in real sense to keep required social distancing required for such patients (Physical Distancing) and in additionally IoT could be easy solution for monitoring and controlling function of such ventilator those could be adjusted with the help of various buttons electronically near the system was emphasized by doctors [8].

C. Robotic Surgery

Robotic surgery pushes boundaries of technical innovation in healthcare in pursuit of better clinical results [9]. In robotic surgeries doctor deploys a small IoT device connected robots that is inserted into human body who perform complex procedure of surgery which reduce the size of incisions which used to be big earlier but because of IoT is less invasive process, faster and recovery and healing is faster of patients as old surgeries were complex as in certain cases it was difficult to manage operation using hands to reach certain areas of our body which lead to large incisions. Today's procedures and specialties use robotic surgical systems, including cardiology, urology, endocrinology, metabolic, and bariatric surgery, head and neck surgery, and all intra-abdominal surgical subspecialties [9].

D. Smart Beds

IoMT that is growing in innovation and medical devices now hospital beds have become smart beds with monitor's patient's various medical requirements data points ranging from checking on the weight, body temperature, electronically updation of patient's medical records with all data when the patient is hospitalized, checking on heartbeats, blood, oxygen level, pressure sensors etc. The system keeps a record of the patient's smart bed image using an IP camera and sensory data from five key points of the patient's body, that is, heart rate, blood pressure, body temperature, motion detector, and bed occupancy [10], [11], [12], [13]. Apart from this the smart beds also keep a check on patients' movements like how many times he/she left the bed or how often they had turned in their bed. Further they have features like alarm or vocal voice alerts that triggers as soon as patient's wanting to go out of bed for example, 'please don't get up'.

Bioengineering /Biomedical engineering when interfaced with technology has changed healthcare sector in developed countries to certain extent but it will take time to be at par with technologies for developing countries. Certain developing countries in private hospitals these facilities are provided but there are concerns about misuse of technology, various legal concern surround around the validity of certain biomedical/bioengineering techniques and IoMT.

IV. INTERNET OF MEDICAL DEVICES AND PRACTICAL CHALLENGES OF TECHNOLOGICAL GAPS

Regardless of development of bioengineering integrated with technology and shown advancement in treatment and diagnosis, medical IoMT still not legalized or not considered a routine practice by many professionals. IoMT is not legally acceptable or enforceable due to the regulation by law and governing bodies on basis of concern which are based on ethical grounds, and technological challenges due to individual personal rights, therefore, of the growth of medical IoT is prevented in many countries. Though healthcare technology is uncritically viewed as a way of achieving better efficiencies of care in many technology implementation projects, and its implementation is thought of as a standardized process, through which technology packages can 'drop into' routine use [14]. IoMT which is technology based will less human intervention by medical practitioners and staff and dependence on technological receivers or patients who become or treated as passive users of those devices and his needs are taken care by the defined technology developers instead of doctors or medical staff [14]. Technology cannot be full proof, and there may be error in the device which could be fatal to the patients' health if the data are not recorded correctly by the IoMT device as it functions automatically as per the settings done and error happened in those devices could see unforeseeable risk to the health. Many a time the kind of service guaranteed by the hospitals and the service provided is seen to be mismatch between promises of health technology said by the hospital professionals and the reality is way too away from the promises that had been seen and highlighted through various studies [14].

Biomedical engineering through it advance technological usage has transformed healthcare sector. IoT technology through wearable devices that had been heavily used and had contributed to advancing the healthcare system through monitoring through devices but at the same

time had raised concerns that would affect the monitoring system healthcare industry. These concerns include (1) failing to use real-time data in the monitoring systems during testing of application, (2) battery issues, (3) security and privacy of the data collected from patients, (4) requirement of medical professional's recommendations at each step of the development, (5) clinical validation or experts' acceptability, and (6) user friendliness for the patients and for healthcare professionals [6]. The failure of real time data in the monitoring period when the device is on testing mode application can give erroneous information, electronic wearable devices those run through charging many a times face battery issues that could lead to complications for patient in case of emergencies or certain ailments. Privacy of the patient's data and security is another important concern for the patient and from legal perspective because the data when transferred to the doctor also store in the server of the system which have third parties' access could be tampered or misused and also exposed to other hospital staff which leads to major privacy concerns issues. Next concern of patient health care is pertaining to intervention and requirement of doctor's recommendation that could be needed is serious health cases at each step and development that taking place at patients end, so we cannot solely rely on the devices for treatment for long periods of time. The data transferred by the patient to the doctor or through devices are not verified by the doctors or professionals and these are not clinically verified and validated and are these data acceptable in all cases of ailments and diseases. Lastly these wearable devices or medical devices are concern on usability and raises the question, 'Are these devices user friendly for the patient for all segment of patients?' educated people could adapt and learn quick but what about elderly, illiterate and techno phobic people, children etc. can they use it as required. Not only this many healthcare professionals are not user friendly to such devices.

Several recent studies across the world concluded that the healthcare system sector suffers from a serious lack of available personnel, and healthcare experts carry a heavy burden of labour during the whole process [10]. Such kind of situations where in health care professionals totally rely on such devices for treatment will further decline overall medical attention and requirement of doctor at particular time for those patients who are sick. Additionally, research demonstrates that the healthcare industry is under a significant amount of strain that is already developed, in addition to those that are still developing. During the time of Covid-19 pandemic the situation of doctors had been experience around the world wherein doctor presence decline due to social distancing and consultation through virtual mode that had shown the side effects of technological side.

V. LEGAL REGULATORY CHALLENGES OF INTERNET OF MEDICAL THINGS (IOMT)

Legal system monitoring play's important role in regulating the functioning of any system and therefore, healthcare sector is also regulated by regulatory bodies, laws, rules, regulations, and guidelines provided from time-to time. Legal compliances and regulation also lay down potential barriers that had restricted and prevented IoMT from being adopted uniformly in the healthcare sector. Law regulates the operating models of the hospital and clinics, alert about the issues of data breaches of patient's information or confidentiality issues, shortage of trained, skilled, and equipped digital talents amongst doctors and their IT staff. Another restriction or prevention could be seen through patients' comfortability and their lack of understanding of medical devices or wearables and their personal information sharing with other people apart from doctor make them uneasy and have confidentiality issues. IoT devices, services & software, and the communication channels that connect them are at risk of attack by a variety of malicious parties, from novice hackers to professional criminals and even state actors (Code of practice for securing consumer internet of things (IoT). (n.d.)). Due to extensive growth of IoMT devices in the healthcare sector and industries it has become difficult to ensure the data privacy and security of the information of the patients and does it comply with the end points compliance specified by the authorities on safety and security of patients information and data based on provided standardize rules and guidelines that the regulating authority passed or ordered to protect the end term user of such biomedical IoMT devices and networks that are used to connect with such IoMT devices by all the stalk holders from doctors, staff, hospital, service providers and server security.

With the emergence of Artificial Intelligence (AI) that is extensively could extensively be used in future and that it is anticipated that there is future growth of IoMT devices that are used in medical treatment and diagnosis, it is essentially important at the end of doctors and hospitals utilizing IoMT for their patient to ensure that they follow the prescribed points of compliance of safety standards and security standards those are provided or ordered as per rules and regulation to secure and protect the users of such devices and also the network providers to maintain confidentiality. The global internet of things in healthcare market was valued at $113.75 billion in 2019 and is expected to reach $332.67 billion by 2027, registering a

CAGR of 13.20% 2020-2027 (What is internet of Medical Things (IoMT) security? (n.d.)). These IoMT has huge prospect in future due to the healthcare sector large usage, however, at the same time the healthcare sector would become the foremost target for cyber security attacks by the attackers those are major concern with all medical devices that would become vulnerable for attack and would provide the information or data to cyber criminals who could misuse such data for their malicious actions. These IoMT devices used in healthcare sectors are significantly at risk and jeopardising the patient's data which would be at risk that could affect his or her safety, misuse of data or data breach for different purposes, those devices could be affected by using ransomware, or malware attacks which could be risk for the patient. Not only this but such devices could be hijacked to affect the hospital's reputations and also affect patient also. Moreover, these devices could be seen to comply with regulatory compliances that is major problem seen in healthcare sector that need to be regularized through standard practices.

Another concern with Biomedical devices used through IoMT differs as per there functionality that are subject to different specification and levels of security varies from device to device and risk associated with them can differ on the kind of IoMT device and the data collected of the patient based on its security risk varies. Therefore, it needs to be identified and recognized the security risk level for each IoMT devices that need to be classified into categories depending upon privacy and security risk associated with such IoMT devices application in healthcare sector. Such IoMT data of patients through the devices could be at risk of Cybersecurity issues that could be misused by breaching the information that could be risky or fatal to the patient's life or could be misused for unauthorised purpose without patient's informed consent. Depending on the risk associated them has to be assessment for patient's IoMT devices. Apart from security, the privacy of the data of the individuals is another very important domain, especially in sectors like health care (Code of practice for securing consumer internet of things (IoT). (n.d.)).

The data security, security risk and privacy are important expect in medical healthcare sector depending on for what purpose the patient's information is being used where the information or data could be intentionally or unintentionally leaked by the someone from the healthcare sector or connected to the healthcare sector for example, a server provider in whose server cloud the data is stored could unintentionally leaked data due to ineffective security control at various stages that could lead to consequences not known to anyone. Therefore, it is important for the healthcare sector those are using IoMT devices for their patients for providing such services need to have placed the security risk assessment and provide security design at the very outset keeping all the foreseeable consequences into mind and also complying all data security measures, protection of cyber security attacks, malicious privacy and data breaches etc. by following standards practices and following guidelines of authorities. Nowadays IoMT devices become very much popular and due to which lots of concern on data privacy and security of data privacy was in question.

VI. IOMT SECURITY BEST PRACTICES EMERGENCE AND DEVELOPMENT ACTIONS NEED OF TIME

Due to issues of data privacy and security that healthcare sector faced for long time since the emergence to IoT and emerging technologies adaption by health industry was always at risk of data breaches, privacy and confidentiality concerns and there was not regulatory rules or law to regulate the same. The first globally applicable standard for consumer IoT was released by TC CYBER in February 2019 and was developed into ETSI EN 303 645, released in June 2020 [15]. This standard that is laid for all types of consumer protection is designed in such a way that it will prevent large-scale of cyber security attacks that are done by predators against smart devices which will at the very beginning will create a model standard rule for the connected all consumer products and further also has futuristic IoT schemes that provide certifications. This entire system of standard rules for cyber security in IoT are inbuilt in the smart devices itself to avoid the hiccup of cyber security issues faced by different IoT devices. These have 13 standard recommendations as per ETSI EN 303 645 that has been supported by good security standards from the manufacturer and vendors themselves and being set on certain rules which has features as no default passwords option, laying down of the way by which implementation of vulnerabilities issues and disclosure policies beforehand with informed consent format and mandatory for IoT devices to keep their software devices updated with latest version to avoid cyber-attacks and also has standard specific rules for data protection norms when exposed to consumer IoT devices those are being followed and accepted by many countries across the globe for IoT. These recommendations of cybersecurity are not applicable for healthcare sectors that being clearly mentioned but following the footsteps of cybersecurity measures healthcare sector need to take necessary preventative measures for security of IoMT devices.

Medical healthcare sectors are using IoMT at a larger

pace and use smart devices for treatment and diagnosis it mandatory for them to follow now IoMT best practices that will provide security to all stakeholders. Healthcare sectors need to take security of all connected clinical and medical devices seriously placing their security strategies and implementation of IoT recommendations with robust implementation of cyber security to avoid all sort of cyber-attacks. Once the standardize strategies are followed and security measures placed then the medical professional that use IoMT clinical or medical devices could focus on most on the welfare and care of patients giving them better outcomes through treatment and diagnosis. For best IoMT security strategies following figure will explain the things that need to be taken care by the healthcare sector while using IoMT devices.

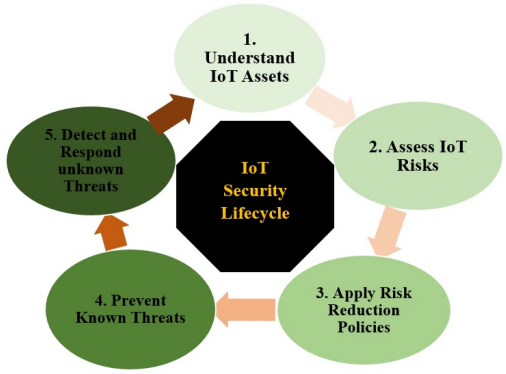

Fig. 1. The IoT security lifecycle is an approach that organizations can use to reduce exposure to cybersecurity threats related to medical devices on their networks (What is internet of Medical Things (IoMT) security? (n.d.).).

IoMT security system need to me Robustic that would ensure the risk assessment of such devices and how many devices are connected at a time that could be of medical one or operation healthcare devices at a time should be clearly specified and each of the device so connected should have specific identity policies to trace them done in case of tampering, hacking or breach through whatever sources. In the healthcare sector wherever IoMT devices applicable whether medical or operational they should be regulated and used as per policies that has to put in place before hand prior to exposure of utilization of such devices. Application of such devices should be through contextual network segmentation and minimum people in the hospital should have access to it, those having access much be skilled to have knowledge to use them and take necessary precautionary measures to avoid cybersecurity issues or data leakage. Whenever IoMT devices exposed for treatment or diagnosis by hospitals to its patients that should be monitor at regular intervals how the device performs and whenever necessary and required to take measure to protect data breaches should take required step for known and unknown threats during monitoring periods. Technologies though little bite technical but the process of management and usage of such devices could be simplified through time-to-time training and updating the operational functions of devices to the person who has access of operation of such IoMT devices. As specified in the above figure the healthcare sector or hospitals can follow the IoMT security approach cycle and take adequate step as per the stage of the happening of event.

VII. PREVENTIVE MEASURES FOR REGULATING AND PROTECTING IOMT IN HEALTHCARE SECTOR

Apart from the above cycle the persons authorized to use or who is being given access to such medical and operational devices should be trained and updated about such device usages and in case of threat what should be he/she could immediately do in case of threat to reduce the damage of cyberthreat or data breaches should be trained or made aware as per the requirement and type of device that is utilized. Following points also could be done:

- Hospitals and clinics should know which devices are IoMT, how to manage them, in case of not use how to secure them through proper process of unmanaged devices, what sort of device they are by categorizing them in by ways of clinical devices or nonclinical devices or operational devices.
- Prior to utilizing any IoT device the risk should be assessed well, and they should be monitored whenever they are used at regular intervals depending on the device type.
- Hospitals need to have at place policies that demarcate the roles and responsibilities of usage and how they could be enforceable only to authorized behaviour and misuse could lead to action against the perpetrator.
- From time-to-time keep update system of IoMT devices and take precautionary measures in advance to prevent any kind of known IoT attacks that are prevalent to such devices.
- Through continuous monitoring and risk assessment IoMT threats could be timely detected and resolved by necessary action.
- Follow the IoMT security lifecycle that will help in managing IoMT devices of all kinds.

VIII. CONCLUSION

Biomedical Engineering through IoMT has widely adapted in medical healthcare sector but there is speculation that relating to the safety, security and privacy of

the patients that need to be addressed due to absence of standardized practices and protocols in various countries and also various in case of developed and developing countries when come to IoMT devices that has protective gaps for patient's privacy and hospitals may face issues of cybersecurity attacks. Though healthcare sector is having very strict regulatory measures pertaining to the normal regulation but it has not develop the same way in case of biomedical when linked with IoMT which has concerns of patients' health security and safety of such medical devices could be compromised because IoMT that is not has so far consolidated standardized protocols or policies which is comprehensive that could assess the risk and lay down security strategies for protection of sensitive nature of information stored in devices, server and clouds. As compared to IoT which is much regularized through set protocols and standardization policies that is not case of IoMT devices. IoMT in healthcare needs to fix these regulatory gaps that is not developed yet which could precisely detect known and unknown threats and preventive measures could be taken to respond such cybersecurity threats or any kind of suspicious medical devices where in the communication could be compromised. Technological IoMT in healthcare sector need to set up standardized security protocols and policies like code of ethics for medical professionals across IoMT devices to handle and resolve all intricate cybersecurity efforts. IoMT has huge potential therefore, healthcare sector and policymakers need to setup varying levels of safety, preventive and security measures to implement uniform and robust protective actions that could fill the security gaps faced by IoMT.

REFERENCES

[1] Z. O. Abu-Faraj, *Handbook of research on biomedical engineering education and advanced bioengineering learning: interdisciplinary concepts: interdisciplinary concepts*. IGI Global, 2012, vol. 2.

[2] J. D. Bronzino, *Biomedical Engineering Fundamentals*, 1st ed. Boca Raton, 2006.

[3] J. D. B. John D. Enderle, Susan M. Blanchard, *Introduction To Biomedical Engineering*, 2nd ed. Elsevier Academic Press, 2005.

[4] S. Sittadjody, T. Criswell, J. D. Jackson, A. Atala, and J. J. Yoo, "Regenerative medicine approaches in bioengineering female reproductive tissues," *Reproductive Sciences*, vol. 28, no. 6, pp. 1573–1595, 2021.

[5] C.-Y. Kuo, H. Baker, M. H. Fries, J. J. Yoo, P. C. Kim, and J. P. Fisher, "Bioengineering strategies to treat female infertility," *Tissue Engineering Part B: Reviews*, vol. 23, no. 3, pp. 294–306, 2017.

[6] P. Kakria, N. Tripathi, and P. Kitipawang, "A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors," *International journal of telemedicine and applications*, vol. 2015, pp. 8–8, 2015.

[7] V. Yeri and D. Shubhangi, "Iot based real time health monitoring," in *2020 Second international conference on inventive research in computing applications (ICIRCA)*. IEEE, 2020, pp. 980–984.

[8] I. H. A. S. F. E. F. Mashoedah, Umi Rochayati and A. Nuryanto, "Iot enabled ventilator monitoring system for covid-19 patients," *Journal of Physics*, 2021.

[9] B. Sakshi and S. S. Pathak, "Robotic surgery: A narrative review," *Cureus*, vol. 14, no. 9, 2022.

[10] S. Ayouni, M. Maddeh, S. Al-Otaibi, M. B. Alazzam, N. M. Alturki, and F. Hajjej, "Development of a smart hospital bed based on deep learning to monitor patient conditions," *Journal of Disability Research*, vol. 2, no. 2, pp. 25–36, 2023.

[11] Gov.UK. (2018) Code of practice for consumer iot security. [Online]. Available: https://shorturl.at/tuCD4

[12] Paloalto. (2022) What is internet of medical things (iomt) security? [Online]. Available: https://shorturl.at/bjlAE

[13] H. Hyndøy, "Cyber security in the cellular internet of things," Master's thesis, NTNU, 2022.

[14] F. Chang, S. Kuoppamäki, and B. Östlund, "Integrating personal emergency response systems (pers) into healthcare professional practices: A scoping review," in *International Conference on Human-Computer Interaction*. Springer, 2020, pp. 28–46.

[15] (2024) Consumer iot security. [Online]. Available: https://shorturl.at/btLU4